



# ความปลอดภัยบนโลกออนไลน์

ดร.ชาลี วรกุลพิพัฒน์

CISSP, CISA

หัวหน้าห้องปฏิบัติการวิจัยความมั่นคงปลอดภัยไซเบอร์ (CSL)

หน่วยวิจัยไร้สาย ข้อมูลความมั่นคงและนวัตกรรมอิเล็กทรอนิกส์ เพื่ออนุรักษ์  
พลังงานและสิ่งแวดล้อม (WISRU)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

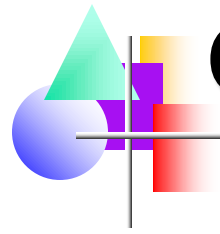
[Chalee.vorakulpipat@nectec.or.th](mailto:Chalee.vorakulpipat@nectec.or.th)



## ดร.ชาลี วรกุลพิพัฒน์

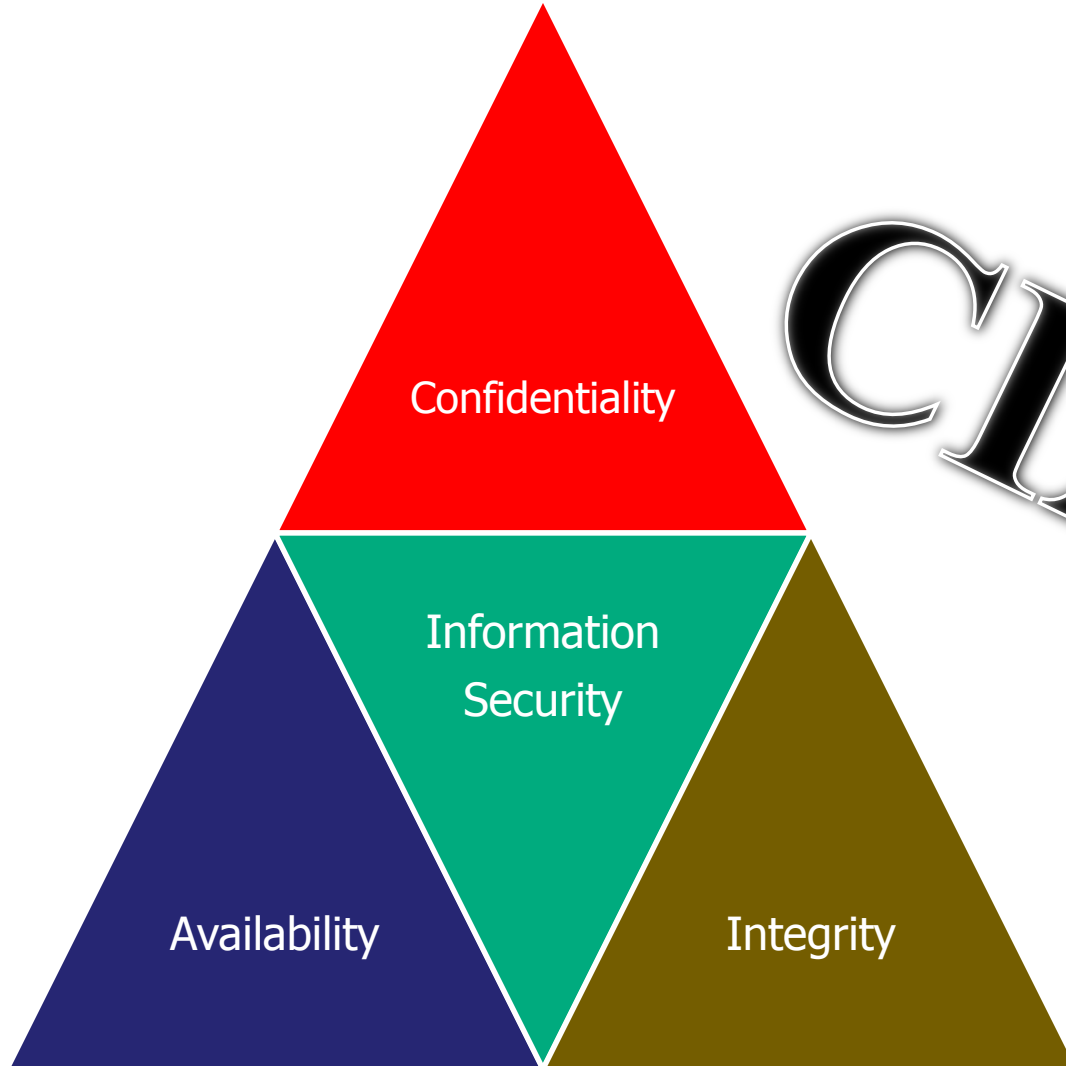
- ประวัติการศึกษา
  - PhD (Information Systems) University of Salford ประเทศอังกฤษ
  - วท.ม. (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยเกษตรศาสตร์
  - วศ.บ. (อิเล็กทรอนิกส์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- ประวัติการทำงาน
  - หัวหน้าห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) (2540-ปัจจุบัน)
  - อนุกรรมการและเลขานุการ คณะอนุกรรมการมั่นคงปลอดภัย ภายใต้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ (2552-ปัจจุบัน)
  - หัวหน้า ThaiCERT (2553-2554)
  - อาจารย์พิเศษ (เกษตรศาสตร์, ศรีปทุม, ธุรกิจบัณฑิต, พระนครเหนือ)
  - วิทยากรบรรยายพิเศษให้หน่วยงานภาครัฐและเอกชน

- Certificate: CISSP, CISA, IRCA ISMS Lead Auditor ISO/IEC 27001
- รางวัลและเกียรติยศ
  - NECTEC Star 3 ครั้ง (2553,2555,2556)
  - รางวัลแนวคิดวิจัยและพัฒนา (ชมเชย) กสท โทรคมนาคม ในงานวิจัย Green Email: อีเมลไร้สแปม 2554
  - รางวัลวิทยานิพนธ์ดีเยี่ยม (ชนะเลิศ) สาขาเทคโนโลยีสารสนเทศและนิเทศศาสตร์ สภาวิจัยแห่งชาติ 2552
  - Outstanding Paper Award (Highly Commended), Journal of Knowledge Management 2552
  - Featured Student, Informatics Research Institute, University of Salford 2549
  - ทุน ก.พ. (กระทรวงวิทย์) ศึกษาต่อในระดับปริญญาเอก 2547
- บทความวิชาการ ต่างประเทศ 23 บทความ ในประเทศ 7 บทความ
- แต่งหนังสือ "UML ภาษามาตรฐานเพื่อผู้พัฒนาซอฟต์แวร์" ซีเอ็ดยูเคชั่น



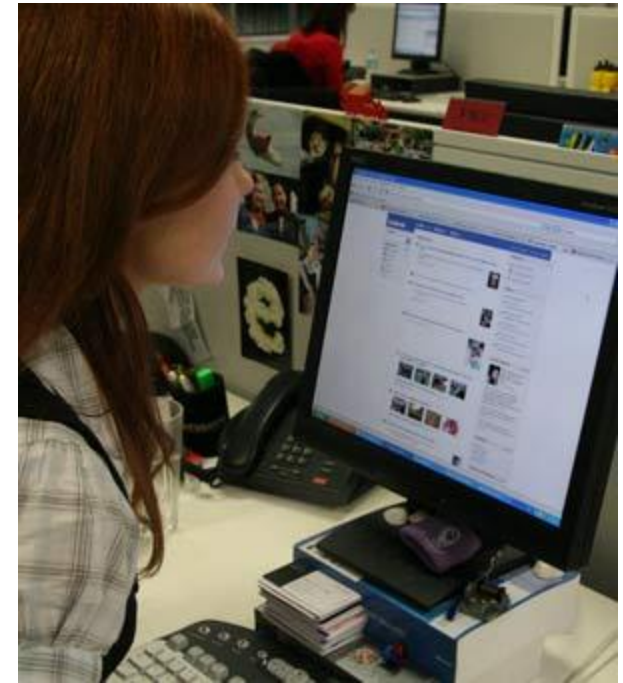
# CIA ของหน่วยงาน

---



CIA

# ทำไมต้องคำนึงถึง security



# Facebook as a Diary

- บอกว่าเราทำอะไร อยู่ที่ไหน
- การโพสต์ข้อความเชิญชวนให้ขโมยเข้าบ้าน

The screenshot shows a Facebook post from Jon W.T. Liang. The post features a photo of a bowl of beef curry with a bun. The text of the post is in Thai: "ตุ๋นตุ๋นแล้ว... กับ Wei-En Ma ที่ 初和風精緻咖哩". Below the photo, there are comments. One comment is in Thai: "ตุ๋นตุ๋นแล้ว... กับ Wei-En Ma ที่ 初和風精緻咖哩". Another comment is in English: "Dear Yosef, this is just a simple Japanese beef curry, and it's not so tasty as it looks...". The post also has a timestamp: "10 ธันวาคมที่แล้ว · ถูกใจ".



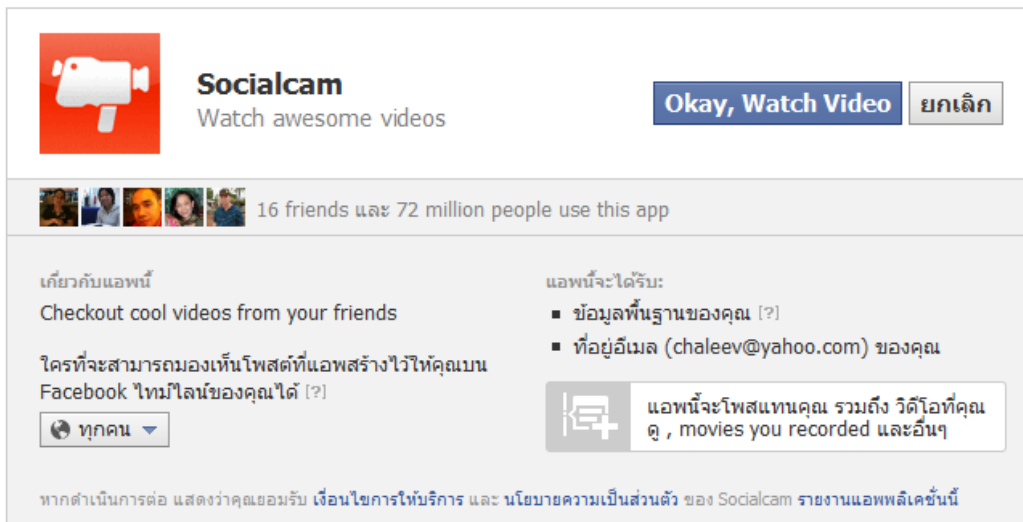
# Facebook as a Data Storage

- ข้อมูลที่โพสต์ลงบนอินเทอร์เน็ต อาจถูกเก็บอยู่ในนั้นได้เป็นสิบๆ ปี อาจเป็นหลักฐานทางกฎหมายได้



# Facebook knows what we are DOing

- เรากำลังดูข้อมูลอะไร คนอื่นทราบหมด
- ***"The more function an application has, the less secure it tends to be,"*** Roger Thompson, chief research officer for AVG



**Socialcam**  
Watch awesome videos

Okay, Watch Video ยกเลิก

16 friends และ 72 million people use this app

เกี่ยวกับแอปนี้  
Checkout cool videos from your friends

ใครที่จะสามารถมองเห็นโพสต์ที่แอปสร้างไว้ให้คุณบน Facebook ใหม่นี้ของคุณได้ [?]

ทุกคน ▾

แอปนี้จะได้รับ:

- ข้อมูลพื้นฐานของคุณ [?]
- ที่อยู่อีเมล (chaleev@yahoo.com) ของคุณ

แอปนี้จะโพสต์แทนคุณ รวมถึง วิดีโอที่คุณดู , movies you recorded และอื่นๆ

หากดำเนินการต่อ แสดงว่าคุณยอมรับ เงื่อนไขการให้บริการ และ นโยบายความเป็นส่วนตัว ส่วนตัว ของ Socialcam รายงานแอปพลิเคชันนี้



กิจกรรมล่าสุด

Thep ได้เป็นเพื่อนกับ Krit Krittanat แล้ว

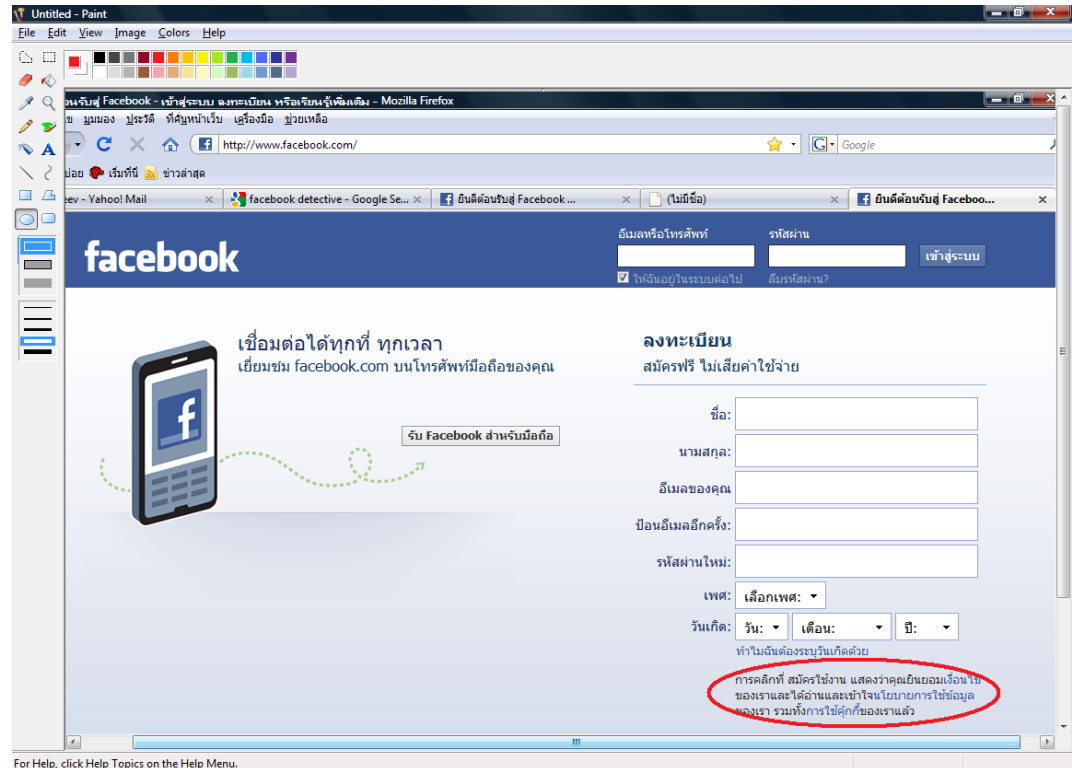
Thep ดู เห็นมากกกกก!!!! บน Socialcam ถูกใจ · แสดงความคิดเห็น

Thep ถูกใจ ตัน ภาสกรนที



# Terms & Conditions

- เราเคยได้อ่านหรือเปล่า
- หรือเราโกหกกว่าอ่านแล้ว
- **BIG LIAR!!!!**





# Spam Hoax

---

- Spam Hoax ผ่านกลุ่มต่างๆ ใน Social Network
- ข้อมูลใน Facebook ถูกส่งผ่านเร็วกว่าสื่ออื่นๆ
- การ Unsubscribe Spam ประโยชน์หรือโทษ???

# Phishing/Virus/Malware thru Facebook

- หลายคนรู้จักวิธีหลีกเสี่ยง Phishing/Virus/Malware เป็นอย่างดี แต่ตกเหยื่อด้วยวิธี Short URL (เช่น bit.ly) ผ่าน Facebook
- แก่ด้วยวิธี Preview

## Expand URL



Title: [Giveaway] 5 Daniusoft Video Converter Ultimate Lifetime Licenses up For Grabs [Worth \$300 - Winners Announced]

Short URL: <http://bit.ly/boQpKY>

Redirects: 1 ([hide details](#))

1. <http://virgintech.org/giveaway-win-5-free-license-for-daniusoft-video-converter-ultimate.html>

Long URL: <http://virgintech.org/giveaway-win-5-free-license-for-daniusoft-video-converter-ultimate.html>

## Extra Info

Meta Keywords: Giveaway Daniusoft Video Converter Ultimate Licenses

Meta Description: 5 Daniusoft Video Converter Ultimate Lifetime licenses to be given away for free in this Contest/Giveaway.

Content-Type: text/html; charset=UTF-8

## Browse with Confidence and Increased Security!

Avoid phishing, malware, and viruses by examining short URLs before visiting them. Find out where links take you.



# CAPTCHA

---

- Facebook อาจให้ผู้ที่โพสต์ URL link ไปยัง Wall ของคนอื่นต้องตอบคำถาม CAPTCHA ก่อน เพื่อมั่นใจว่าผู้ส่งไม่ใช่ Machine Spammer
- Re-CAPTCHA???

**Security Check**

**Security Check:**  
Enter both words below, separated by a space.  
Can't read the words below? Try different words or an audio captcha.



Sick of these? [Verify your account.](#)

Text in the box:  [What's This?](#)

# การป้องกัน

## ■ Balance

- Technical vs Non-Technical Issues
- Security vs Ease of Use or Convenience
- ท่านจะทำอย่างไร ถ้าวันหนึ่งผู้บริหารของท่านสั่งห้ามใช้ Facebook หรือ Youtube

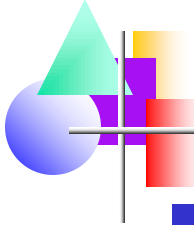




# ไม่เปิดเผยข้อมูลส่วนตัว

---

- เมื่อกรอกข้อมูลส่วนตัวลงพวก **Facebook** เราต้องทราบก่อนว่าผู้ใดจะสามารถเห็นได้บ้าง เฉพาะเพื่อน เพื่อนของเพื่อน หรือใครก็ได้
- ในยุค **Web 2.0 Hacker** สามารถขโมยข้อมูลเพื่อนำไปขายหรือใช้ประโยชน์ทางธุรกิจได้

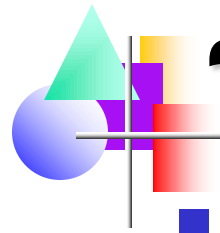


# ส่งสัยไว้ก่อน

---

- อย่าเชื่อข้อมูลใน **Social Network** จนเกินไป ควรจะส่งสัยไว้ก่อนว่าข้อมูลนั้นน่าเชื่อถือ มีประโยชน์หรือไม่





# ระวังก่อนพิมพ์

---

- ทุกอย่างที่คุณพิมพ์ลงไป อาจย้อนกลับมาหาตัวคุณได้ โดยเฉพาะการโพสต์พฤติกรรมที่ไม่ค่อยดีลงไป



# ทำตัวเหมือนฝ่ายบุคคล

---

- หากคุณกำลังติดต่อกับคนแปลกหน้าผ่าน **Social Network** คุณต้องทราบให้ได้ก่อนว่าคนๆ นั้นที่แท้จริงคือใคร เหมือนใช้ระบบสกรีนคนตอนสมัครงาน



# ระวังเป็นพิเศษตอน **On the Move**

---

- หากกำลังใช้ **Social Network** บนโทรศัพท์มือถือ จะเพิ่มความเสี่ยง
- คำนึงเรื่อง **Location-based Service**
- สมบัติล้ำค่า 3 อย่างอาจถูกขโมยในเวลาเดียวกัน –
  - โทรศัพท์มือถือ
  - ข้อมูลข้างใน
  - ตัวตน



# กลับไปอ่าน Terms & Conditions

---

- หากยังมีข้อสงสัย ให้กลับไปอ่าน Terms & Conditions ให้ดี โดยเฉพาะ Privacy Policy
- หากไม่เห็นด้วย ก็ไม่ควรใช้



# กรณีศึกษา

---





# จำกัดการเข้าถึง

---

- ใน USA และ UK ตามสถาบันการศึกษาหรือห้องสมุดพยายามที่จะจำกัดการใช้งานเนื่องจาก MySpace กลายเป็น **“such a heaven for student gossip and malicious comments”** และ MySpace ใช้ internet bandwidth กว่า 40% ในหนึ่งวันในการใช้เว็บ ทำให้ internet ช้าลง



# ปัญหาเรื่อง Profile

---

- สร้างความเสียหายแก่นักเรียนเอง: มีรายงานว่าใน **USA** นักเรียนส่วนใหญ่มักใส่ **profile** ที่ดูสูงหรือดู **over** เกินไป ลงใน **MySpace** ของตนเอง นายจ้างอาจไม่พิจารณาบุคคลแบบนี้





# การจำกัดอายุ $\geq 14$ ปี

---

- คนที่อายุ 14-15 จะถูกกำหนด profile ให้เป็น private
- 16 หรือมากกว่า จะให้เลือกสิทธิในการเข้าถึงได้
- เด็กจะถูกจำกัดการเข้าถึงข้อมูลที่ไม่เหมาะสม เช่น sex contents
- ในปี 2006 เด็กวัยรุ่นหญิงฆ่าตัวตาย อันเนื่องมาจากการถูกกลั่นแกล้งและใส่ความจากเพื่อนวัยรุ่นชายคนหนึ่ง ใน MySpace ซึ่งแท้จริงแล้ววัยรุ่นชายคนนั้นไม่มีตัวตนจริง แต่เป็นการปลอมตัวโดยแม่ของเพื่อนของเหยื่อ
  - <http://www.foxnews.com/story/0,2933,312018,00.html>
  - [http://en.wikipedia.org/wiki/Suicide\\_of\\_Megan\\_Meier](http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier)



WIKIPEDIA The Free Encyclopedia

- Main page
- Contents
- Featured content
- Current events
- Random article
- Donate to Wikipedia

- Interaction
  - Help
  - About Wikipedia
  - Community portal
  - Recent changes
  - Contact Wikipedia

Toolbox

Print/export

Languages

- Español
- Italiano
- Portugués

Article Talk

Read Edit View history

Search

# Suicide of Megan Meier

From Wikipedia, the free encyclopedia

**Megan Taylor Meier** (November 6, 1992 – October 17, 2006) was an American teenager from [Dardenne Prairie, Missouri](#), who committed **suicide** by [hanging](#) three weeks before her fourteenth birthday. A year later, Meier's parents prompted an investigation into the matter and her suicide was attributed to [cyber-bullying](#) through the [social networking](#) website [MySpace](#). The mother of a friend of Meier, [Lori Drew](#), was later indicted on the matter in 2008, but in 2009, Drew was acquitted.<sup>[1]</sup>

## Contents [hide]

- 1 Background
- 2 Death
- 3 Investigation
  - 3.1 Local
  - 3.2 Federal
- 4 Reactions
- 5 See also
- 6 References
- 7 External links

## Background

[edit]

Megan Meier was born in [O'Fallon, Missouri](#), to Christina "Tina" Meier and Ronald Meier. She had lived in nearby [Dardenne Prairie](#) during her childhood, with her parents and sister Allison.

From the third grade, Megan had been under the care of a [psychiatrist](#). She had been prescribed [citalopram](#), [methylphenidate](#) and

### Megan Meier



Megan Meier

<b>Born</b>	Megan Taylor Meier November 6, 1992 O'Fallon, Missouri, U.S.
<b>Died</b>	October 17, 2006 (aged 13) Dardenne Prairie, Missouri, U.S.
<b>Cause of death</b>	<a href="#">Suicide by hanging</a>
<b>Resting place</b>	Saint Charles Memorial Gardens



# ประเด็นอื่นๆ ในกรณีศึกษา

---

- ลิขสิทธิ์เพลง สังคม วัฒนธรรม กฎหมาย
- Google ขอใส่ช่อง search ลงในเว็บไซต์ MySpace ซึ่ง **MySpace** จะได้ประโยชน์หรือเสียผลประโยชน์?

# กรณีศึกษา: Security Failure



ASSOCIATED PRESS

Olatunji Oluwatosin, a Nigerian national accused of stealing personal information from people through bogus accounts with ChoicePoint Inc., pleaded no contest last week in Los Angeles Superior Court. The company disclosed yesterday how many people in each state may have been victimized.



# Hacker

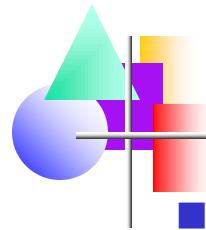
---

- **White-hat hackers**

- มีจรรยาบรรณ ตรวจสอบระบบเพื่อหาช่องโหว่ เพื่อจะได้แก้ไข

- **Black-hat hackers**

- เป็น cracker ที่ทำลาย ก่อปัญหา



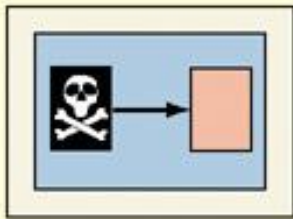
# ตัวอย่างการภัยคุกคาม

---

- **Virus**
- **Worm**
- **Spyware**
- **DoS**
- **Phishing**
- **Botnet**
- **Spam**

# ไวรัสคอมพิวเตอร์ทำงานอย่างไร

Just as a biological virus disrupts living cells to cause disease, a computer virus—introduced maliciously—invades the inner workings of computers and disrupts normal operations of the machines.



**1** A virus starts when a programmer writes a program that embeds itself in a host program.



**2** The virus attaches itself and travels anywhere that the host program or piece of data travels, whether on floppy disk, local area networks, or bulletin boards.

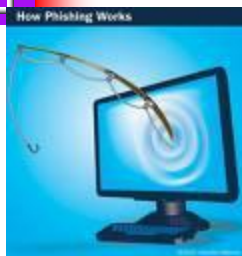


**3** The virus is set off by either a time limit or some set of circumstances, possibly a simple sequence of computer operations by the user (e.g., open an attachment). Then it does whatever the virus programmer intended, whether it is to print "Have a nice day" or erase data.





# Phishing




Account Information - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: HSW Bank.com Sent: Fri 11/25/2005 2:04 PM  
To: John Doe  
Cc:  
Subject: Account Information

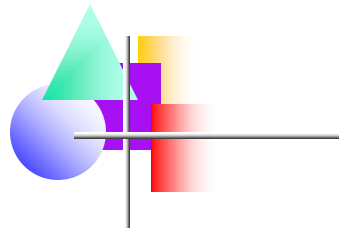


Dear customer:

During an automated audit on 11/20/2005, we discovered discrepancies in your account. Please follow the link below to confirm your account information with us. Failure to respond within five business days will result in the termination of your account.

Sincerely, HSW Bank

<http://hswbank.accountmaintenance.com/verify/0984325.htm>



Remember, Old National will never send you emails asking for your personal and/or financial information.

From: ID-protection@Oldnationalbank.com  
Date: 8/5/2005 2:57 PM  
Subject: Important Account Information ( Unusual login attempts - Case ID:1234567)

Dear Old National Bank Customer,

We recently noticed several attempts to log in to your personal account from a foreign IP address and we have reason to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you.

The login attempt was made from:  
IP address: 123.45.123.45  
ISP Host: cache-66.proxy.aol.com

After three unsuccessful attempts to access your account, your personal Online Profile has been locked. This has been done to secure your accounts and to protect your private information. We are trying to make sure that your online transactions are secure.

You must unlock your profile by going to:

This is not Old National's url

<http://www.Oldnationalbank.com/index.html>

Be extremely cautious about clicking on links provided within emails.

If you should have any additional questions or concerns, please contact Customer Service at: [service@Oldnationalbank.com](mailto:service@Oldnationalbank.com)

Thank you for using OldnationalBank! 2005 Oldnationalbank Corporation. All rights reserved. Equal Opportunity Lender. Member FDIC.

Be wary of overall poor grammar & misspellings.

# Phishing

The image shows a screenshot of a MySpace website page designed to look like a phishing site. The browser's address bar displays a legitimate URL: `http://205.188.226.153/sohal201/myspace.com`. The page header features the MySpace logo and navigation links. A prominent message reads "You Must Be Logged-In to do That!". Below this, a text box displays a different URL: `http://123.456.789.012/sohal201/myspace.com`. The main content area contains a "Member Login" form with fields for "E-Mail" and "Password", a "Remember Me" checkbox, and a "LOGIN" button. A red error message states "Your session has expired. Please re-login." A larger, semi-transparent white box with a blue border is overlaid on the page, containing the same error message and login form, effectively obscuring the original page content. At the bottom, there are links for "About", "FAQ", "Terms", "Privacy", "Safety Tips", "Contact MySpace", "Promote!", "Advertise", and "MySpace International", along with a copyright notice for 2003-2006 MySpace.com.

http://205.188.226.153/sohal201/myspace.com

Help

**myspace.com**  
a place for friends

The Web MySpace Search Help | SignUp

You Must Be Logged-In to do That!

MySpace is FREE, But Feature

`http://123.456.789.012/sohal201/myspace.com`

Your session has expired. Please re-login.

**Member Login**

E-Mail :

Password :

Forgot your password?

Remember Me

Not a MySpace Member? Join FREE!

After You Sign Up You Can:

- Create Free Profiles on MySpace
- Upload Pictures & Write Blogs
- Use MySpace Mail & Instant Messenger

**Your session has expired!**

Your session has expired. Please re-login.

**Member Login**

E-Mail :

Password :

Forgot your password?

Remember Me

[About](#) | [FAQ](#) | [Terms](#) | [Privacy](#) | [Safety Tips](#) | [Contact MySpace](#) | [Promote!](#) | [Advertise](#) | [MySpace International](#)

©2003-2006 MySpace.com. All Rights Reserved.

## Example of a typical, poorly-constructed phishing e-mail message

**From...** UTSA MAINTENANCE <maintenace@utsa.edu>  
**To...** John Doe  
**Cc...**  
**Subject:** MAINTENANCE ALERT!!

Dear Email User,

Prior to the unwanted spam in our UTSA webmail service, we have decided to perform mentainance on our site. Our mentainance is based on free Anti-spamming protection for all UTSA users account, which is number 10 of our UTSA email/exchange terms and condition. You are to send in your information below in this order.

\*\*\*\*\* **Reputable organizations / companies will NEVER ask for your password** \*\*\*\*\*

1.) FULL NAME:  
2.) USER ID:  
3.) PASSWORD:  
4.) ALTERNATE EMAIL:  
5.) SECRET QUESTION:  
6.) SECRET ANSWER:  
7.) DATE OF BIRTH:

\*\*\*\*\*

This process will help us to fight against spam mails. Failure to submit your UTSA email/exchange Account Details, will render your email address in-active from our database.

NOTE: You will be notifield in your email password reset message immediately after undergoing this process for security reasons.

Technical System Team

[MAINTENANCE TEAM  
maintenance@utsa.edu](mailto:maintenance@utsa.edu) <mailto:maintenance@utsa.edu>

**misspelled words / poor grammar**

**E-mail address should be "Office of Information Technology"**

The diagram includes several callouts: a red box labeled "misspelled words / poor grammar" with arrows pointing to "maintenace" in the sender address, "mentainance", "account", and "terms and condition" in the body text; a blue box labeled "Reputable organizations / companies will NEVER ask for your password" with an arrow pointing to "PASSWORD:" in the list; and another blue box labeled "E-mail address should be 'Office of Information Technology'" with arrows pointing to the sender address and the "mailto:" link at the bottom.

# BotNet

## ตัวอย่างการใช้ BotNet ในการส่ง spam mail





# เราจะป้องกันอย่างไร?

---

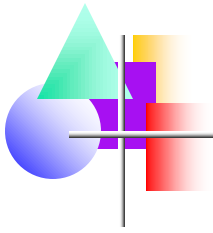
- มีมาตรการป้องกันที่ดี เช่น มีระบบป้องกันไม่ให้คนที่ไม่ได้มีสิทธิเข้าถึงข้อมูล (login/password)
- มีระบบตรวจจับการบุกรุก เช่น Anti-virus
- จำกัดความเสียหายให้น้อยลง เช่น มี fault-tolerant system เพื่อให้ระบบพอจะใช้งานได้ไปก่อน (degraded mode)
- หาวิธีทำให้ระบบกลับคืนสู่สภาพปกติ เช่น มีแผนที่จะแก้ไขปัญหาให้เร็วที่สุดในกรณีที่เกิดความเสียหายต่อระบบ ต้องพิจารณาระหว่าง replace กับ repair
- สร้างความตื่นตัว (awareness) เช่น ออกกฏนโยบาย หรือ มีการฝึกอบรม IT security



# สรุปการใช้คอมพิวเตอร์ให้ปลอดภัย

---

- ใช้สามัญสำนึก (Common sense) แม้จะไม่รู้รายละเอียดของกฎหมาย หรือ ไม่รู้ว่ามีความหมายนั้นด้วยหรือไม่
- การบุกรุก โจมตี ถือว่าผิดกฎหมาย
- แม้ว่าจะไม่ทำอะไรเลยก็อาจผิดกฎหมายได้ เช่น ถ้าท่านมีหน้าที่ป้องกัน แต่ละเลย
- มีจริยธรรมไว้ก่อน
- ศึกษาอย่างต่อเนื่อง



---

**ขอบคุณครับ**